# *National Cyber Infrastructure Protection Act of 2010*

The National Cyber Infrastructure Protection Act of 2010 sets clear lanes in the road to protect our nation's cyber security, but leaves flexibility for the private sector and Government to adapt to changing threats. It places the Federal Government's cyber security effort under the strategic and budgetary control of the Director of the National Cyber Center and establishes a Cyber Defense Alliance to encourage voluntary cooperation by the private sector in protecting private sector and critical infrastructure information networks against cyber attack. This coordinated approach is vital to improving our national cyber defenses across the entire cyber spectrum.

***National Cyber Center.*** The Act establishes a National Cyber Center, housed within the Department of Defense for administrative purposes only. The missions of the National Cyber Center include serving as the primary organization for coordinating Federal Government defensive operations, cyber intelligence collection and analysis, and activities to protect and defend Federal Government information networks; providing a process for resolving inter-agency conflicts; and ensuring that Federal agencies have access to cyber threat information, including appropriate private sector information. The Act requires the Secretaries of Defense and Homeland Security, the Director of National Intelligence, and the Director of the Federal Bureau of Investigation to collocate and integrate within the Center such elements necessary to carry out the Center's missions. Other Federal agencies may also participate in the Center. The Act calls for integration of cyber-related information, including databases with such information.

***Director of the National Cyber Center.*** The Act creates a Senate-confirmed Director of the National Cyber Center who shall serve for a term not to exceed 5 years and may not simultaneously serve in any other capacity in the Executive branch. The Director reports directly to the President, but his position may not be located within the Executive Office of the President. The Director's duties include coordinating Federal Government cyber activities to protect and defend Federal Government information networks; acting as the President's principal adviser on such matters; and developing policies for securing Federal Government information networks and sharing cyber threat-related information among Federal agencies and with the private sector. The Act creates a National Cyber Security Program, similar to the National Intelligence Program which funds Intelligence Community activities, and requires that the Director coordinate and ensure the adequacy of Federal agency Program budget requests.

***Cyber Defense Alliance.*** The Act establishes within a National Laboratory a public-private partnership to facilitate the flow of cyber threat and technology information between the private sector and the Government. Initially funded by the Government, the Alliance members will assume primary funding responsibility, with the Government's annual contribution not to exceed 15% of operating costs. A Board of Directors, consisting primarily of private sector representatives, will determine rules and procedures for membership. The Alliance will be the clearinghouse for passing sensitive cyber threat information to those businesses and entities on the front lines of cyber attacks. The Act provides important exemptions from FOIA and antitrust restrictions. The Alliance has a set duration, ceasing to exist on December 31, 2020, unless otherwise extended by Congress.